Office of Information Technology
Policy

Remote Access to Internal Networks

Policy:
Agencies that allow remote access to their internal networks via desktop PC's and laptops must ensure these devices are configured as indicated by IT STD 1-15.

Scope:
This policy is applicable to all entities under the authority of the Office of Information Technology, pursuant to the provisions of R.S. 39:15.1, et seq.

Responsibilities:
- Agencies are required to develop policies and procedures that address the requirements of this policy.
- Blackberry/PDA devices and "smart phones," due to their fast-paced technological advances, are not within the scope of this policy. However, agencies must assess and take the necessary steps to mitigate the security risks associated with these devices.
- Relative to development and support contracts, agencies are required to include specific contract language that requires the contractor to adhere to OIT Security Policies and Standards if there is need for remote access to the agency's internal network.
- Where applicable, agencies are required to utilize existing enterprise standards.
- Agencies should pursue the use of "health-check" software that determines the status (whether or not anti-virus and firewall software are loaded with the latest updates) of remote PC's and laptops before they are allowed access to the internal network.
- Agencies should develop an implementation plan detailing the steps required to become compliant with this policy.
- Where possible, agencies should plan to migrate from direct-dial access to broadband connectivity.

Related Policies, Standards, Guidelines:
IT STD 1-15 *Remote Access to Internal Networks*

Owner:
OIT Security Office

Effective Date:
July 27, 2009